

EXTREMAL PRODUCT-ONE FREE SEQUENCES IN $C_q \rtimes_s C_m$

F. E. BROCHERO MARTÍNEZ AND SÁVIO RIBAS

ABSTRACT. Let G be a finite group, written multiplicatively. The Davenport constant of G is the smallest positive integer d such that every sequence of G with d elements has a non-empty subsequence with product 1. Let $C_n \simeq \mathbb{Z}_n$ be the cyclic group of order n . In [1], J. Bass showed that the Davenport constant of the metacyclic group $C_q \rtimes_s C_m$, where q is a prime number and $\text{ord}_q(s) = m \geq 2$, is $m + q - 1$. In this paper, we explicit the form of all sequences S of $C_q \rtimes_s C_m$, with $q + m - 2$ elements, that are free of product-1 subsequences.

1. INTRODUCTION

Given a finite group G written multiplicatively, the *Zero-sum Problems* study conditions to ensure that a given sequence in G has a non-empty subsequence with prescribed properties (such as length, repetitions, weights) such that the *product* of its elements, in some order, is equal to the identity of the group.

One of the first problem of this type is the remarkable Theorem of Erdős-Ginzburg-Ziv (see [4]): Given $2n - 1$ integers, it is possible to select n of them, such that their sum is divisible by n , or in group theory language, every sequence S with $l \geq 2n - 1$ elements in a finite cyclic group of order n has a subsequence of length n , the product of whose n elements being the identity. In this theorem, the number $2n - 1$ is the smallest integer with this property.

Traditionally, this class of problems have been extensively studied for abelian groups. We can see overviews of Zero-sum Theory for finite abelian groups in the surveys of Y. Caro [3] and W. Gao and A. Geroldinger [7].

An important type of Zero-sum Problem is to determine the *Davenport constant* of a finite group G (written multiplicatively): This constant, denoted by $D(G)$, is the smallest positive integer d such that every sequence with d elements in G (repetition allowed) contains some subsequence such that the product of its terms in some order is 1.

For $n \in \mathbb{N}$, let $C_n \simeq \mathbb{Z}_n$ denote the cyclic group of order n written multiplicatively. The Davenport constant is known for some groups, such as:

- $D(C_n) = n$;
- $D(C_m \times C_n) = m + n - 1$ if $m|n$ (J. Olson, [14]);
- $D(C_{p^{e_1}} \times \cdots \times C_{p^{e_r}}) = 1 + \sum_{i=1}^r (p^{e_i} - 1)$ (J. Olson, [13]);
- $D(D_{2n}) = n + 1$ where D_{2n} is the Dihedral Group of order $2n$ (see [15] and [20]);
- $D(C_q \rtimes_s C_m) = m + q - 1$ where $q \geq 3$ is a prime number and $\text{ord}_q(s) = m \geq 2$ (J. Bass, [1]).

However, it is still open for most other groups.

By the definition of the Davenport constant, there exist sequences S of G with $D(G) - 1$ elements that are free of *product-1 subsequences*, i.e, there exists $S = (x_1, \dots, x_{D(G)-1})$ sequence of G such that $x_{i_1} x_{i_2} \cdots x_{i_k} \neq 1$ for every non empty subset $\{i_1, i_2, \dots, i_k\} \subset \{1, 2, \dots, D(G) - 1\}$. The *Inverse Zero-sum Problems* study the structure of these extremal sequences which are free of product-1 subsequences with some prescribed property. Some overviews on the inverse problems can be found in articles such as [9], [17] and [8].

The inverse problems associated to the Davenport constant are already solved for a few abelian groups. The following theorem resolves the issue for the group C_n .

Theorem 1.1 ([9, Theorem 2.1]). *Let S be a sequence in C_n free of product-1 subsequences, where $n \geq 3$. Suppose that $|S| \geq (n + 1)/2$. Then there exists some $g \in S$ with multiplicity $\geq 2|S| - n + 1$. In particular, if $|S| = n - 1 = D(C_n) - 1$ then $S = (\underbrace{g, \dots, g}_{n-1 \text{ times}})$, where g is a generator of C_n .*

Observe that in the cyclic case, sequences free of product-1 subsequences contain an element repeated many times. It is natural to ask if this is true in a general case. Specifically, let us say that a given finite abelian group G has *Property C* if every maximal sequence S which is free of product-1 subsequences with at most $\exp(G)$

Date: November 1, 2016.

2010 *Mathematics Subject Classification*. 20D60 (primary) and 11P70 (secondary).

Key words and phrases. Zero-sum problem, Davenport constant, inverse zero-sum.

elements, i.e. the exponent of the group G , has the form

$$S = (\underbrace{T, T, \dots, T}_{\exp(G)-1 \text{ times}}),$$

for some subsequence T of S . The above theorem states that C_n has the Property C. It follows from a result of C. Reiher in [16] that C_p^2 possesses Property C (see also [9] and [6]). In [8], W. Gao, A. Geroldinger and D. J. Grynkiewicz showed that this result is multiplicative, extending this result for C_n^2 where n is a composite number. In [18], W. A. Schmid discusses the case $C_n \times C_m$, where $n|m$. Not much is known about groups of rank ≥ 3 , only few specific cases (see, for example, [18]).

A *minimal zero sequence* S in a finite abelian group G is a sequence such that the product of its elements is 1, but each proper subsequence is free of product-1 subsequences. In [5, Theorem 6.4], W. Gao and A. Geroldinger showed that if $|S| = D(G)$ then S contains some element $g \in G$ with order $\text{ord}(g) = \exp(G)$ for certain groups such as p -groups, cyclic groups, groups with rank two and groups that are the sum of two elementary p -groups. They also conjectured that the same conclusion holds for every finite abelian group.

Another type of inverse zero-sum problem, associated to the Erdős-Ginzburg-Ziv Theorem, was proved by A. Bialostocki and P. Dierker in [2]. They established that if S is a sequence in C_n with $2n - 2$ elements and S is free of product-1 subsequences with n elements, then

$$S = (\underbrace{g, \dots, g}_{n-1 \text{ times}}, \underbrace{h, \dots, h}_{n-1 \text{ times}})$$

for some $g, h \in C_n$ with $\text{ord}(gh^{-1}) = n$.

In this article, we characterize the maximal sequences which are free of product-1 subsequences for certain non-abelian groups and we show that these sequences have a property similar to Property C. Let q be a prime number, $m \geq 2$ be a divisor of $q - 1$ and $s \in \mathbb{Z}_q^*$ such that $\text{ord}_q(s) = m$. Denote by $C_q \rtimes_s C_m$ the *metacyclic group* $\mathbb{Z}_q \rtimes_s \mathbb{Z}_m$ written multiplicatively, i.e., the group generated by x and y with relations:

$$x^m = 1, \quad y^q = 1, \quad yx = xy^s, \quad \text{where } \text{ord}_q(s) = m. \quad (1.1)$$

Specifically, we prove the following result:

Theorem 1.2. *Let q be a prime number, $m \geq 2$ be a divisor of $q - 1$ and $s \in \mathbb{Z}_q^*$ such that $\text{ord}_q(s) = m$, where $(m, q) \neq (2, 3)$. Let S be a sequence in the metacyclic group $C_q \rtimes_s C_m$ with $m + q - 2$ elements. The following statements are equivalent:*

- (i) S is free of product-1 subsequences;
- (ii) For some $1 \leq t \leq q - 1$, $1 \leq i \leq m - 1$ such that $\gcd(i, m) = 1$ and $0 \leq \nu_1, \dots, \nu_{m-1} \leq q - 1$,

$$S = (\underbrace{y^t, y^t, \dots, y^t}_{q-1 \text{ times}}, x^i y^{\nu_1}, x^i y^{\nu_2}, \dots, x^i y^{\nu_{m-1}}).$$

2. NOTATION

Let G be a finite group written multiplicatively and $S = (g_1, g_2, \dots, g_l)$ be a sequence of elements of G . Suppose that T is a subsequence of S , say $T = (g_{n_1}, g_{n_2}, \dots, g_{n_k})$, where $\{n_1, n_2, \dots, n_k\}$ is a subset of $\{1, 2, \dots, l\}$. We say that T is a *product-1 subsequence* when

$$g_{\sigma(n_1)} g_{\sigma(n_2)} \cdots g_{\sigma(n_k)} = 1$$

for some permutation σ of $\{n_1, \dots, n_k\}$, and if there are no such product-1 subsequences then we say that S is *free of product-1 subsequences*.

Suppose that $S_1 = (g_{i_1}, \dots, g_{i_u})$ and $S_2 = (g_{j_1}, \dots, g_{j_v})$ are subsequences of S . Then

- $\pi(S) = g_1 g_2 \cdots g_l$ denotes the product of the elements in S in the order that they appear;
- $\pi_n(S) = g_{n+1} \cdots g_l g_1 \cdots g_n$, for $0 \leq n \leq l - 1$, denotes the product of the elements in S with a n -shift in the indices;
- $|S| = l$ denotes the length of the sequence S ;
- SS_1^{-1} denotes the subsequence formed by the elements of S without the elements of S_1 ;
- $S_1 \cap S_2$ denotes the intersection of the subsequences S_1 and S_2 . In the case that $S_1 \cap S_2 = \emptyset$, we say that S_1 and S_2 are disjoint subsequences;
- $S_1 S_2 = (g_{i_1}, \dots, g_{i_u}, g_{j_1}, \dots, g_{j_v})$ denotes the concatenation of S_1 and S_2 ;
- $S^k = SS \cdots S$ denotes the concatenation of k identical copies of S 's.

For the group $C_q \rtimes_s C_m = \langle x, y | x^n = 1, y^q = 1, yx = xy^s \rangle$, let

- H be the cyclic subgroup of order q generated by y ;
- $N = (C_q \rtimes_s C_m) \setminus H = N_1 \cup N_2 \cup \cdots \cup N_{m-1}$, where $N_i := x^i H$ for $1 \leq i \leq m - 1$.

From the definition of semi-direct product, $C_q \simeq H \triangleleft (C_q \rtimes_s C_m)$ and $C_m \simeq [(C_q \rtimes_s C_m)/H]$.

3. AUXILIARY RESULTS

In this section we present the auxiliary theorems and lemmas that we use throughout the paper. First, we need the definition of sum-set and product-set:

Definition 3.1. *If X and Y are non-empty subsets of an abelian group G then the sum-set is defined by*

$$X + Y = \{a + b \in G \mid a \in X, b \in Y\}.$$

If G is a non-abelian group, written multiplicatively, then the product-set is defined by

$$X \cdot Y = \{a \cdot b \in G \mid a \in X, b \in Y\}.$$

A very fundamental result on sum-sets is the Cauchy-Davenport Theorem, which gives a lower bound for the number of elements of a sum-set in \mathbb{Z}_q depending on the cardinality of each set.

Theorem 3.2 (Cauchy-Davenport inequality, [12, p. 44-45]). *For q a prime number and for any r non-empty sets $X_1, \dots, X_r \subset \mathbb{Z}_q$,*

$$|X_1 + \dots + X_r| \geq \min\{q, |X_1| + \dots + |X_r| - r + 1\}.$$

Looking at the inequality above in the case that $r = 2$ we get $|X + Y| \geq \min\{q, |X| + |Y| - 1\}$. A pair of subsets X, Y of \mathbb{Z}_q is called a *critical pair* if the equality $|X + Y| = \min\{q, |X| + |Y| - 1\}$ occurs. The following theorem provides criteria for a pair $X, Y \subset \mathbb{Z}_q$ to be a critical pair.

Theorem 3.3 (Vosper, [19]). *Let q be a prime number and let X, Y non-empty subsets of \mathbb{Z}_q . Then*

$$|X + Y| = \min\{q, |X| + |Y| - 1\}$$

if and only if one of the following conditions is satisfied:

- (a) $|X| + |Y| > q$;
- (b) $\min\{|X|, |Y|\} = 1$;
- (c) $|X + Y| = q - 1$ and $Y = \mathbb{Z}_q \setminus \{c - a \mid a \in X\}$, where $\{c\} = \mathbb{Z}_q \setminus (X + Y)$;
- (d) X and Y are arithmetic progressions with the same common difference.

Notice that assertion (a) above is the only one giving the equality $|X + Y| = q$, that is, $X + Y = \mathbb{Z}_q$. Assertion (b) means that we just translate the set Y , supposing $|X| = 1$. The non-trivial cases yielding a critical pair are (c) and (d).

Now, suppose that A is a sequence in $C_q \rtimes_s C_m$ and that A has no elements in the normal subgroup H , but that the product of its elements is in H . The next lemma shows that if A is minimal with these properties then it is possible to generate at least $|A|$ distinct products in H , just shifting the order of the product.

Lemma 3.4. *Let $A = (a_1, a_2, \dots, a_l)$ be a sequence in $N \subset C_q \rtimes_s C_m$, where $\text{ord}_q(s) = m$, such that $\pi(A) \in H$ but no subsequence of A has product in H . Then:*

- (a) $\pi_n(A) \in H$ for every $0 \leq n \leq l - 1$;
- (b) $\pi_i(A) \neq \pi_j(A)$ for every $0 \leq i < j \leq l - 1$.

Proof: This proof is contained in the proof of Lemma 14 in [1]. □

Throughout this paper, we deal with many expressions of the type $a_0 + a_1s + \dots + a_{m-1}s^{m-1} \pmod{q}$, where $a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_q$. The following lemma explains why we can assume without loss of generality that this kind of expression has a value different than 0 under a weak assumption.

Lemma 3.5. *Let $A = (a_0, a_1, \dots, a_{m-1})$ be a sequence in \mathbb{Z}_q with at least 2 distinct elements, say $a_i \not\equiv a_j \pmod{q}$. Suppose that $\text{ord}_q(s) = m$. Then*

$$\sum_{k=0}^{m-1} a_k s^k \not\equiv a_i s^j + a_j s^i + \sum_{\substack{k=0 \\ k \neq i, j}}^{m-1} a_k s^k \pmod{q}.$$

In particular, if one of them is 0 modulo q then the other is not 0 modulo q .

Proof: Since at least two elements are distinct, there exists $0 \leq i \leq m-1$ such that $a_i \not\equiv a_{i+1} \pmod{q}$ (assuming that the index of the coefficients are taken modulo m , i.e., $a_0 = a_m$). Since $\text{ord}_q(s) = m$, we may translate the coefficients by multiplying by s , therefore we may assume without loss of generality that $i = 0$, i.e., $a_0 \not\equiv a_1 \pmod{q}$. Now, if

$$\sum_{k=0}^{m-1} a_k s^k \equiv a_0 s + a_1 + \sum_{k=2}^{m-1} a_k s^k \pmod{q}$$

then

$$a_0 + a_1 s \equiv a_1 + a_0 s \pmod{q} \iff (a_0 - a_1)(1 - s) \equiv 0 \pmod{q},$$

a contradiction. \square

One of the assertions from Vosper's Theorem says that if X and Y are arithmetical progressions then X and Y form a critical pair. On the other hand, if $\alpha = a_0 + a_1 s + \dots + a_{m-1} s^{m-1} \in \mathbb{Z}_q$ then the set $\{\alpha s^j\}_{j=0,1,\dots,m-1}$ is a geometric progression. Since we have the freedom to choose the order of the products, it is expected to deal with critical pairs that are formed by geometric progressions. The following lemma shows under some conditions that, in \mathbb{Z}_q , an arithmetic progression can not be a geometric progression.

Lemma 3.6. *Let $q \geq 5$ be a prime number, $s \in \mathbb{Z}_q^* \setminus \{1\}$ and $2 \leq k \leq q-1$. Let*

$$\mathcal{A} = \{1, 2, 3, \dots, k-1\},$$

$$\mathcal{B} = \{k, k+1, k+2, \dots, q-1\}$$

be two sets of classes modulo q . Then \mathcal{A} and \mathcal{B} are not invariant by multiplication by s .

Proof: Since \mathcal{A} and \mathcal{B} are complementary in \mathbb{Z}_q^* , they are both s -invariants or not simultaneously. Suppose that they are s -invariants.

As $1 \cdot s \in \mathcal{A}$ and $(q-1) \cdot s \in \mathcal{B}$, we obtain $2 \leq s \leq \min\{k-1, q-k\}$, therefore we may assume without loss of generality $k-1 \leq q-k$. So $2 \leq s \leq k-1 \leq (q-1)/2$. Let $c \equiv s^{\text{ord}_q(s)-1} \pmod{q}$ be the inverse of s modulo q . Since $s^j \in \mathcal{A}$ for all $j \in \mathbb{N}$ and $s \not\equiv 1 \pmod{q}$, we obtain $c \in \mathcal{A}$ and $c \not\equiv 1 \pmod{q}$, thus $c-1 \in \mathcal{A}$, which implies $s \cdot (c-1) \equiv 1-s \in \mathcal{A}$. But $1-s$ has a representative in \mathcal{B} , which is a contradiction. \square

The next lemma gives both upper and lower bounds for the number of solutions $(z, w) \in \mathbb{Z}_q^2$ of the equation $az^2 - bw^4 \equiv c \pmod{q}$ when $q \equiv 1 \pmod{4}$ and $a, b \in \mathbb{Z}_q^*$ are fixed. We use the upper bound to show that the set $\{c + bw^4 \mid w \in \mathbb{Z}_q^*\}$ contains both quadratic and non-quadratic residues modulo q .

Lemma 3.7. *Let $q \equiv 1 \pmod{4}$ be a prime number, $a, b, c \in \mathbb{Z}_q^*$ and N the number of solutions $(z, w) \in \mathbb{Z}_q^2$ of $az^2 - bw^4 \equiv c \pmod{q}$. Then*

$$|N - q| < 3\sqrt{q}.$$

Proof: Direct consequence of Theorem 5 page 103 in [11]. \square

Corollary 3.8. *Let $q \equiv 1 \pmod{4}$ be a prime number such that $q \geq 13$ and let $b, c \in \mathbb{Z}_q^*$. Then there exist $w_1, w_2 \in \mathbb{Z}_q^*$ such that $c + bw_1^4$ is a quadratic residue and $c + bw_2^4$ is a non-quadratic residue.*

Proof: Fix $a \in \mathbb{Z}_q^*$ and denote by N the number of solutions of

$$az^2 - bw^4 \equiv c \pmod{q}. \quad (3.1)$$

Let $w_0 \in \mathbb{Z}_q^*$ such that $\text{ord}_q(w_0) = 4$. Since each solution of equation (3.1) generates seven other solutions (by switching z by $-z$ and multiplying w by powers of w_0), the number of elements in the set

$$\mathcal{C} = \{az^2 \mid z \in \mathbb{Z}_q^*\} \cap \{c + bw^4 \mid w \in \mathbb{Z}_q^*\}$$

is at most $N/8$. By the previous lemma, it follows that

$$|\mathcal{C}| < \frac{q + 3\sqrt{q}}{8} < \frac{q-1}{4} = |\{c + bw^4 \mid w \in \mathbb{Z}_q^*\}|,$$

therefore

$$\{c + bw^4 \mid w \in \mathbb{Z}_q^*\} \not\subset \{az^2 \mid z \in \mathbb{Z}_q^*\}.$$

Thus, selecting a being either a square or not, we obtain that the set $\{c + bw^4 \mid w \in \mathbb{Z}_q^*\}$ contains quadratic residues and non-quadratic residues. \square

It follows from the corollary above and Lemma 3.5 that, in the case $m = (q-1)/2$, it is possible to get more than the m distinct values which were provided by Lemma 3.4.

Corollary 3.9. *Let $q \equiv 1 \pmod{4}$ be a prime number such that $q \geq 13$, $s \in \mathbb{Z}_q^*$, such that $\text{ord}_q(s) = \frac{q-1}{2} = m$ and $a_0, a_1, \dots, a_{m-1} \in \mathbb{Z}_q$. Suppose that each of the sets*

$$\{a_0, a_2, a_4, \dots, a_{m-2}\} \text{ and } \{a_1, a_3, a_5, \dots, a_{m-1}\}$$

has at least two distinct elements modulo q . Then the set

$$\mathcal{A} = \{a_{\sigma(0)} + a_{\sigma(1)}s + a_{\sigma(2)}s^2 + \dots + a_{\sigma(m-1)}s^{m-1} \in \mathbb{Z}_q \mid \sigma \text{ is a permutation of } (0, 1, \dots, m-1)\}$$

has at least $q-1$ distinct elements.

Proof: By Lemma 3.5, we can suppose without loss of generality that

$$\alpha := a_0 + a_1s + a_2s^2 + \dots + a_{m-1}s^{m-1} \not\equiv 0 \pmod{q}.$$

Notice that we can obtain αs^j by shifting the coefficients, so $\alpha s^j \in \mathcal{A}$ for all $0 \leq j \leq m-1$. By Lemma 3.4, these m elements are distinct.

Since $\text{ord}_q(s) = (q-1)/2$, s is a square modulo q and, indeed, s generates the quadratic residues modulo q , therefore the elements αs^j are all quadratic residues or all non-quadratic residues depending on whether α is a square or not. Define

$$b \equiv a_1s + a_3s^3 + \dots + a_{m-1}s^{m-1} \pmod{q},$$

$$c \equiv a_0 + a_2s^2 + \dots + a_{m-2}s^{m-2} \pmod{q}.$$

In the same way, by Lemma 3.5 we can assume without loss of generality that $b, c \not\equiv 0 \pmod{q}$. Since $c + bs^{2j} \in \mathcal{A}$ for all $0 \leq j \leq m/2$, Corollary 3.8 tells us that the set $\{c + bs^{2j} \mid 0 \leq j \leq m/2\}$ contains a quadratic residue and a non-quadratic residue modulo q . By multiplying by s , we obtain all quadratic residues and all non-quadratic residues modulo q . Therefore, $|\mathcal{A}| \geq q-1$. \square

Analogously to the previous corollary but now in the case $m = q-1$, the next result states that it is possible to split the coefficients into parts such that each part generates at least m distinct values, also improving the result of Lemma 3.4.

Corollary 3.10. *Let $q \equiv 1 \pmod{4}$ be a prime number such that $q \geq 13$, s be a generator of \mathbb{Z}_q^* and $a_0, a_1, \dots, a_{q-2} \in \mathbb{Z}_q$. Suppose that each of the sets*

$$\{a_0, a_4, a_8, \dots, a_{q-5}\}, \{a_1, a_5, a_9, \dots, a_{q-4}\}, \{a_2, a_6, a_{10}, \dots, a_{q-3}\} \text{ and } \{a_3, a_7, a_{11}, \dots, a_{q-2}\}$$

has at least two distinct elements modulo q . Then each of the sets

$$\mathcal{A}_e = \{a_{\sigma(0)} + a_{\sigma(2)}s^2 + a_{\sigma(4)}s^4 + \dots + a_{\sigma(q-3)}s^{q-3} \in \mathbb{Z}_q \mid \sigma \text{ is a permutation of } (0, 2, 4, \dots, q-3)\},$$

$$\mathcal{A}_o = \{a_{\tau(1)}s + a_{\tau(3)}s^3 + a_{\tau(5)}s^5 + \dots + a_{\tau(q-2)}s^{q-2} \in \mathbb{Z}_q \mid \tau \text{ is a permutation of } (1, 3, 5, \dots, q-2)\}$$

have at least $q-1$ distinct elements.

Proof: This follows directly from the previous corollary. \square

4. SEQUENCES IN $C_5 \rtimes_s C_m$

In our proof of Theorem 1.2, for the case $q \equiv 1 \pmod{4}$, we use Corollaries 3.9 and 3.10, where the hypothesis $q \geq 13$ is necessary. In this section, we consider the remaining case, i.e., $q = 5$. There are two possibilities for m , namely, $m = 2$ and $m = 4$.

For $m = 2$ the only possible value for s is 4 (mod 5), therefore we obtain the Dihedral Group of order 10. The next proposition deals with this case and shows that if a sequence S is free of product-1 subsequences and satisfies some assumptions then S must contain an element in H , the normal subgroup.

Proposition 4.1. *Let S be a sequence in $C_5 \rtimes_4 C_2$ free of product-1 subsequences and suppose that $|S| = 5$. Then $S \cap H \neq \emptyset$.*

Proof: Suppose that $S = (xy^{\alpha_1}, \dots, xy^{\alpha_5})$, where $0 \leq \alpha_1 \leq \dots \leq \alpha_5 \leq 4$. If there exist two identical elements in S then their product is 1 and so S is not free of product-1 subsequences. Thus, $(\alpha_1, \dots, \alpha_5) = (0, 1, 2, 3, 4)$, therefore $x \cdot xy^4 \cdot xy \cdot xy^2 = 1$. Hence, S is not free of product-1 subsequences, a contradiction. \square

For $m = 4$, the cases to consider are $s \equiv 2 \pmod{5}$ or $s \equiv 3 \pmod{5}$. The proposition below shows that if S is free of product-1 subsequences then S can not belong to a single coset N_i , where $\text{gcd}(i, 4) = 1$.

Proposition 4.2. *Let $s \in \{2, 3\}$ and let S be a sequence in $C_5 \rtimes_s C_4$ such that $|S| = 7$. If every element of S belongs to a coset N_i , where $i \in \{1, 3\}$, then S is not free of product-1 subsequences.*

Proof: Let $S = (x^i y^{\alpha_1}, \dots, x^i y^{\alpha_7})$, where $i \in \{1, 3\}$ and $0 \leq \alpha_1 \leq \dots \leq \alpha_7 \leq 4$. Notice that at most three of the α_j 's are equal, otherwise the product of four identical elements would be 1. This implies that there are at least three distinct elements. Also, there are at least a pair of elements repeating two or three times. Since $\text{ord}_5(s) = 4$, it follows that $s^{3i_0} + s^{2i_0} + s^{i_0} + 1 \equiv 0 \pmod{5}$. Therefore, for all $\beta \in \mathbb{Z}_q$ it holds that:

$$\begin{aligned} x^{i_0} y^{a_1} \cdot x^{i_0} y^{a_2} \cdot x^{i_0} y^{a_3} \cdot x^{i_0} y^{a_4} &= y^{a_1 s^{3i_0} + a_2 s^{2i_0} + a_3 s^{i_0} + a_4} \\ &= y^{a_1 s^{3i_0} + a_2 s^{2i_0} + a_3 s^{i_0} + a_4 - \beta(s^{3i_0} + s^{2i_0} + s^{i_0} + 1)} \\ &= x^{i_0} y^{a_1 - \beta} \cdot x^{i_0} y^{a_2 - \beta} \cdot x^{i_0} y^{a_3 - \beta} \cdot x^{i_0} y^{a_4 - \beta}, \end{aligned}$$

thus we may assume without loss of generality that the element that repeats most is $\alpha_1 = 0$. If there is another pair of identical elements, say $1 \leq \alpha_j = \alpha_{j+1} = \lambda \leq 4$ for some $3 \leq j \leq 6$, then we may choose $A_1 = (x, xy^\lambda, x, xy^\lambda)$ or $A_1 = (x^3, x^3 y^\lambda, x^3, x^3 y^\lambda)$. Since $\text{ord}_5(s) = 4$ and $\gcd(i, 4) = 1$, it follows that $\lambda s^{2i} + \lambda \equiv 0 \pmod{5}$, and so $x^i \cdot x^i y^\lambda \cdot x^i \cdot x^i y^\lambda = 1$. Otherwise, the only possibility is $(\alpha_1, \dots, \alpha_7) = (0, 0, 0, 1, 2, 3, 4)$ and we may choose, for example,

$$\begin{aligned} A_1 &= (x, x, xy, xy^2) \text{ or } A_1 = (x, x, xy, xy^3) \text{ when } i = 1, \\ A_1 &= (x^3, x^3, x^3 y, x^3 y^2) \text{ or } A_1 = (x^3, x^3, x^3 y, x^3 y^3) \text{ when } i = 3, \end{aligned}$$

as the following table shows:

	$s = 2$	$s = 3$
$i = 1$	$s^i \equiv_5 2 \Rightarrow x \cdot x \cdot xy \cdot xy^3 = 1$	$s^i \equiv_5 3 \Rightarrow x \cdot x \cdot xy \cdot xy^2 = 1$
$i = 3$	$s^i \equiv_5 3 \Rightarrow x^3 \cdot x^3 \cdot x^3 y \cdot x^3 y^2 = 1$	$s^i \equiv_5 2 \Rightarrow x^3 \cdot x^3 \cdot x^3 y \cdot x^3 y^3 = 1$

Thus, S is not free of product-1 subsequences.

5. PROOF OF THEOREM 1.2

In this section we investigate the sequences of $C_q \rtimes_s C_m$ with $m + q - 2$ elements which are free of product-1 subsequences and we prove that an analogue of Property C holds for $C_q \rtimes_s C_m$ provided $\text{ord}_q(s) = m$ and $(m, q) \neq (2, 3)$. Notice that if $(m, q) = (2, 3)$ then $s \equiv 2 \pmod{3}$ and the assertion of Theorem 1.2 is not true for the group $C_3 \rtimes_2 C_2$, which is isomorphic to D_6 , the Dihedral Group of order 6, and to S_3 , the Permutation Group of 3 elements. In fact, the sequence $S = (x, xy, xy^2)$ provides the only counter example when $(m, q) = (2, 3)$.

It is easy to check that (ii) implies (i), therefore we just need to prove that (i) implies (ii). Let us assume that S is a sequence free of product-1 subsequences in $C_q \rtimes_s C_m$. Let us also define $k \in \mathbb{Z}$ by the equation

$$|S \cap H| = q - k.$$

If $k \leq 0$, since $D(H) = D(C_q) = q$, then there exists a product-1 subsequence in H .

If $k = 1$ then $|S \cap H| = q - 1$ and $|S \cap N| = m - 1$. By Theorem 1.1, the elements of $S \cap H$ must all be equal, say, $S \cap H = \{y^t\}^{q-1}$ and the other elements of S must be in the same N_i , where $\gcd(i, m) = 1$.

From now on, assume $k \geq 2$. In this case, we are going to prove that S is not free of product-1 subsequences. We have

$$|S \cap N| = m + k - 2 \geq m = D(C_m) = D((C_q \rtimes_s C_m)/H).$$

Let $A = (a_1, \dots, a_l)$ be a subsequence of $S \cap N$ such that $\pi(A) \in H \simeq C_q$ but no subsequence of A has product in H , as in Lemma 3.4. We have that $2 \leq |A| \leq m$. Let us denote A by A_1 . If $|(S \cap N)A_1^{-1}| \geq m$ then we can construct A_2 with the same property and repeat this argument replacing successively $(S \cap N)(A_1 \dots A_j)^{-1}$ by $(S \cap N)(A_1 \dots A_j A_{j+1})^{-1}$ and so on, until $|(S \cap N)(A_1 \dots A_r)^{-1}| \leq m - 1$. This implies that

$$\sum_{i=1}^r |A_i| \geq |S \cap N| - (m - 1) = k - 1.$$

We construct the following set of products:

$$\begin{aligned} R &= (\{\pi_j(A_1)\}_{j=0,1,\dots,|A_1|-1}) \cdot (\{1\} \cup \{\pi_j(A_2)\}_{j=0,1,\dots,|A_2|-1}) \cdot \dots \\ &\quad \dots (\{1\} \cup \{\pi_j(A_r)\}_{j=0,1,\dots,|A_r|-1}) \subset H. \end{aligned}$$

By the Cauchy-Davenport inequality we obtain

$$|R| \geq \min \left\{ q, |A_1| + \sum_{i=2}^r (|A_i| + 1) - r + 1 \right\} = \min \left\{ q, \sum_{i=1}^r |A_i| \right\}.$$

If this minimum is q then $R = H \ni 1$ and S is not free of product-1 subsequences. On the other hand, if this minimum is $\sum_{i=1}^r |A_i| \geq k - 1$ then we obtain at least $k - 1$ distinct elements in H arising from $S \cap N$. Suppose without loss of generality that $S \cap H = (h_1, h_2, \dots, h_{q-k})$. If $\sum_{i=1}^r |A_i| \geq k$ then, by the Pigeonhole

Principle, either $1 \in R$ or R contains the inverse of one of the products $h_1, (h_1 h_2), \dots, (h_1 \dots h_{q-k})$, hence S is not free of product-1 subsequences.

Therefore, suppose that $\sum_{i=1}^r |A_i| = k - 1$, namely, $R = \{g_1, g_2, \dots, g_{k-1}\}$. If there exist $1 \leq n_1 \leq k - 1$ and $1 \leq n_2 \leq q - k$ such that $g_{n_1} = (h_1 \dots h_{n_2})^{-1}$ then $g_{n_1} h_1 \dots h_{n_2} = 1$ and so S is not free of product-1 subsequences. Therefore,

$$\{g_1, \dots, g_{k-1}, h_1^{-1}, (h_1 h_2)^{-1}, \dots, (h_1 \dots h_{q-k})^{-1}\} = \{y, y^2, \dots, y^{q-1}\}.$$

If $h_i \neq h_j$ for some $1 \leq i < j \leq q - k$, say without loss of generality that $h_1 \neq h_2$, then either the set

$$\{g_1, \dots, g_{k-1}, h_1^{-1}, h_2^{-1}, (h_1 h_2)^{-1}, \dots, (h_1 \dots h_{q-k})^{-1}\}$$

has q elements, in particular, it has the element 1, or it contains two identical elements. In any case, S has a product-1 subsequence. Hence,

$$h_1 = h_2 = \dots = h_{q-k} = y^t$$

for some $1 \leq t \leq q - 1$ and

$$R = \{g_1, g_2, \dots, g_{k-1}\} = \{y^t, y^{2t}, \dots, y^{(k-1)t}\}.$$

Let $C := (S \cap N)(A_1 \dots A_r)^{-1}$. Notice that C is free of subsequences with product in H . Since

$$|C| = |S \cap N| - \sum_{j=1}^r |A_j| = m + k - 2 - (k - 1) = m - 1,$$

we conclude, by Theorem 1.1, that C does not have subsequences with product in H if these $m - 1$ elements are in the same class N_{i_0} , $1 \leq i_0 \leq m - 1$, $\gcd(i_0, m) = 1$. Thus, we assume that C is a sequence in $S \cap N_{i_0}$, namely,

$$C = (x^{i_0} y^{t_1}, x^{i_0} y^{t_2}, \dots, x^{i_0} y^{t_{m-1}}).$$

If there exist $1 \leq j \leq r$ such that A_j has at least one element out of N_{i_0} , then we may select $x^{i_1} y^\theta \in A_j$ with $i_1 \neq i_0$. If $2 \leq l \leq m - 1$ is such that $i_0 l \equiv i_1 \pmod{m}$ then we may replace A_j by

$$\tilde{A}_j = (A_j \setminus \{x^{i_1} y^\theta\}) \cup (x^{i_0} y^{t_1}, \dots, x^{i_0} y^{t_l}),$$

which also has product in H , since

$$\prod_{n=1}^l x^{i_0} y^{t_n} = x^{i_1} y^T$$

for some $T \in \mathbb{Z}_q$ and $H \triangleleft C_q \rtimes_s C_m$. Since $|\tilde{A}_j| > |A_j|$, the new set R generated by this change has more elements. This replacement may mean that \tilde{A}_j is not minimal anymore and in this case we break \tilde{A}_j into its minimal components. Thus,

$$\sum_{\substack{n=1 \\ n \neq j}}^r |A_n| + |\tilde{A}_j| > \sum_{n=1}^r |A_n| = k - 1,$$

therefore there exists a product-1 subsequence in S .

Hence, $S \cap N$ must be a sequence in N_{i_0} , so

$$A_j \pmod{H} = \{x^{i_0}\}^m \quad \text{for all } 1 \leq j \leq r, \text{ and } \quad C = (x^{i_0} y^{t_1}, \dots, x^{i_0} y^{t_{m-1}}).$$

By double counting the number of elements in $S \cap N_{i_0}$ we conclude that $m + k - 2 \equiv m - 1 \pmod{m}$, that is, $k \equiv 1 \pmod{m}$. Since $k \geq 2$ and $k \equiv 1 \pmod{m}$, we have $m + 1 \leq k \leq q$.

Observe that the case $m + 1 \leq k < q$ is not possible. In fact, in this case, if

$$A_j = (x^{i_0} y^{\eta_1}, \dots, x^{i_0} y^{\eta_m})$$

then

$$\pi(A_j) = y^{\eta_1 s^{i_0(m-1)} + \eta_2 s^{i_0(m-2)} + \dots + \eta_{m-1} s^{i_0} + \eta_m}$$

and, more generally,

$$\pi_n(A_j) = \left(y^{\eta_1 s^{i_0(m-1)} + \eta_2 s^{i_0(m-2)} + \dots + \eta_{m-1} s^{i_0} + \eta_m} \right)^{s^{i_0 n}}.$$

We claim that R is invariant under taking powers of s^{i_0} . In fact, since $\gcd(i_0, m) = 1$ we obtain $\text{ord}_q(s^{i_0}) = \text{ord}_q(s) = m$. An element in R is of the form

$$y^{jt} = \pi_{j_1}(A_{\nu_1}) \dots \pi_{j_u}(A_{\nu_u}),$$

where $1 \leq j \leq k - 1$. Taking powers of s^{i_0} in both sides, we obtain that

$$y^{s^{i_0} jt} = \pi_{j_1+1}(A_{\nu_1}) \dots \pi_{j_u+1}(A_{\nu_u})$$

belongs to R , because it can be obtained by the product of some A_i 's in some order. Therefore, the claim is proved.

Looking at the exponent of y , the above claim implies that the set $\{t, 2t, \dots, (k-1)t\}$ is s^{i_0} -invariant modulo q , and so $\{1, 2, \dots, k-1\}$ is s^{i_0} -invariant, which contradicts Lemma 3.6.

From now on, we assume $k = q$ and S is a sequence in N_{i_0} . As $|A_j| = m$ for $1 \leq j \leq r$ and $|C| = m-1$ we obtain $mr + m - 1 = |S| = m + q - 2$, therefore $mr = q - 1$. We consider the following cases depending on whether $r \geq 3$, $r = 2$ or $r = 1$:

- (1) **Case $r \geq 3$:** This implies that $3m \leq q - 1$. Since the equality in the Cauchy-Davenport inequality occurs, Vosper's Theorem with the sets

$$\tilde{A} = \{\pi_n(A_1)\}_n \quad \text{and} \quad \tilde{B} = (\{1\} \cup \{\pi_n(A_2)\}_n) \cdots (\{1\} \cup \{\pi_n(A_r)\}_n)$$

says that at least one of the following statements hold:

- (i) $|\tilde{A}| + |\tilde{B}| > q$;
- (ii) $\min\{|\tilde{A}|, |\tilde{B}|\} = 1$;
- (iii) $|\tilde{A} \cdot \tilde{B}| = q - 1$ and $\tilde{A} = H \setminus \{b^{-1} \mid b \in \tilde{B}\}$;
- (iv) \tilde{A} and \tilde{B} are arithmetic progressions with the same common difference.

Since $|\tilde{A}| + |\tilde{B}| = q$, (i) is not possible, and since $\min\{|\tilde{A}|, |\tilde{B}|\} \geq m \geq 2$, (ii) does not hold. In order to discard item (iii), define

$$\begin{aligned} \tilde{B}_1 &= \{1\} \cup \{\pi_n(A_2)\}_n, \\ \tilde{B}_2 &= (\{1\} \cup \{\pi_n(A_3)\}_n) \cdots (\{1\} \cup \{\pi_n(A_r)\}_n). \end{aligned}$$

As $3m \leq mr = q - 1$, we have

$$\begin{aligned} q - m &= |\tilde{B}| = |\tilde{B}_1 + \tilde{B}_2| = |\tilde{B}_1| + |\tilde{B}_2| - 1 < q - 1, \\ |\tilde{B}_1| &= m + 1, \\ |\tilde{B}_2| &= q - 2m \geq m + 1. \end{aligned}$$

Therefore, the items (i), (ii) and (ii) from Vosper's Theorem are false, hence the exponents of the elements in each of the sets \tilde{B}_1 and \tilde{B}_2 form arithmetic progressions, say

$$\tilde{B}_1 = \{y^{-av}, \dots, y^{-v}, 1, y^v, \dots, y^{(m-a-1)v}\}.$$

Looking at the Vosper's equality involving \tilde{A} and \tilde{B} , item (iii) tells us that \tilde{A} also form an arithmetic progression in the exponent with the same common difference, say

$$\tilde{A} = \{y^w, y^{w+v}, \dots, y^{w+(m-1)v}\}.$$

By switching A_1 and A_2 , the only possibility is that $\{\pi_n(A_1)\} = \{y^v, y^{2v}, \dots, y^{mv}\}$ for some $1 \leq v \leq q - 1$.

On the other hand, the exponents of the elements from the set $\{\pi_n(A_1)\}_n$ are s^{i_0} -invariant, that is, the exponents of y in R are invariant by multiplication by s^{i_0} . By Lemma 3.6, the set $\{\pi_n(A_1)\}_n$ can not be of the above form.

- (2) **Case $r = 2$:** In this case, $m = (q - 1)/2$ and, in particular, s^{i_0} generates the quadratic residues modulo q . The case $(m, q) = (2, 5)$ follows from Proposition 4.1, therefore we may assume $q \geq 7$. If there exist m identical elements then their product is 1, thus there are at most $m - 1$ identical elements. Since

$$\frac{m + q - 2}{m - 1} = \frac{3m - 1}{m - 1} > 3,$$

there are at least 4 distinct elements among $S = \{x^{i_0}y^{\alpha_1}, \dots, x^{i_0}y^{\alpha_{3m-1}}\}$. We split this case into the two subcases $q \equiv 1 \pmod{4}$ and $q \equiv 3 \pmod{4}$.

- (2.1) **Subcase $q \equiv 1 \pmod{4}$ and $q \geq 13$:** We may choose

$$\begin{aligned} A_1 &= (x^{i_0}y^{a_0}, x^{i_0}y^{a_1}, \dots, x^{i_0}y^{a_{m-1}}), \\ A_2 &= (x^{i_0}y^{b_0}, x^{i_0}y^{b_1}, \dots, x^{i_0}y^{b_{m-1}}) \end{aligned}$$

to be disjoint subsequences of S such that it is possible to split each one into two subsequences of the same size, say

$$\begin{aligned} A_1 &= (x^{i_0}y^{a_0}, x^{i_0}y^{a_2}, \dots, x^{i_0}y^{a_{m-2}}) \cup (x^{i_0}y^{a_1}, x^{i_0}y^{a_3}, \dots, x^{i_0}y^{a_{m-1}}), \\ A_2 &= (x^{i_0}y^{b_0}, x^{i_0}y^{b_2}, \dots, x^{i_0}y^{b_{m-2}}) \cup (x^{i_0}y^{b_1}, x^{i_0}y^{b_3}, \dots, x^{i_0}y^{b_{m-1}}), \end{aligned}$$

where each partition has at least 2 distinct elements. This is possible since S has at most $m - 1$ identical elements. From Corollary 3.9, A_1 and A_2 each generate at least $q - 1$ elements in H , therefore the

product-set $A_1 \cdot A_2$ has to be H by the Cauchy-Davenport inequality, which implies that $1 \in A_1 \cdot A_2$. Thus S is not free of product-1 subsequences.

(2.2) **Subcase $q \equiv 3 \pmod{4}$ and $q \geq 7$:** It is known that -1 is not a quadratic residue modulo q . Let

$$\begin{aligned} A_1 &= \{x^{i_0}y^{a_0}, x^{i_0}y^{a_1}, \dots, x^{i_0}y^{a_{m-1}}\}, \\ A_2 &= \{x^{i_0}y^{b_0}, x^{i_0}y^{b_1}, \dots, x^{i_0}y^{b_{m-1}}\}, \end{aligned}$$

where A_1 and A_2 are disjoint subsequences of S and each one has at least 2 distinct elements. It is enough to consider the exponents of y and construct the following sets of exponents:

$$\begin{aligned} X &= \{s^{ni_0}(a_0 + a_1s^{i_0} + \dots + a_{m-2}s^{i_0(m-2)} + a_{m-1}s^{i_0(m-1)}) \in \mathbb{Z}_q \mid 0 \leq n \leq m-1\}, \\ Y &= \{s^{ni_0}(b_0 + b_1s^{i_0} + \dots + b_{m-2}s^{i_0(m-2)} + b_{m-1}s^{i_0(m-1)}) \in \mathbb{Z}_q \mid 0 \leq n \leq m-1\}. \end{aligned}$$

Suppose that $0 \notin X$, $0 \notin Y$ and $0 \notin X + Y$ (otherwise we are done). By Lemma 3.4, $|X| = |Y| = m$. Let

$$\alpha = a_0 + a_1s^{i_0} + \dots + a_{m-2}s^{i_0(m-2)} + a_{m-1}s^{i_0(m-1)} \in X.$$

If $-\alpha \in Y$ then $0 \in X + Y$, a contradiction, therefore $-\alpha \in X$. Hence, there exist $0 \leq n \leq m-1$ such that $\alpha s^{2ni_0} \equiv -\alpha \pmod{q}$, which implies $s^{2ni_0} \equiv -1 \pmod{q}$, so -1 is a quadratic residue modulo q , which is also a contradiction.

(3) **Case $r = 1$:** In this case, $m = q - 1$ and, in particular, m is even and s^{i_0} generates \mathbb{Z}_q^* . The cases where $(m, q) = (4, 5)$ follow from Proposition 4.2, therefore we may assume $q \geq 7$. If there exist m identical elements then their product is 1, thus there are at most $m - 1$ identical elements. Since

$$\frac{m + q - 2}{m - 1} = \frac{2m - 1}{m - 1} > 2,$$

there are at least 3 distinct elements among $S = \{x^{i_0}y^{\alpha_1}, \dots, x^{i_0}y^{\alpha_{2m-1}}\}$. Again, we split up this case into $q \equiv 1 \pmod{4}$ and $q \equiv 3 \pmod{4}$, as follows:

(3.1) **Subcase $q \equiv 1 \pmod{4}$ and $q \geq 13$:** We may choose

$$A_1 = \{x^{i_0}y^{a_0}, x^{i_0}y^{a_1}, \dots, x^{i_0}y^{a_{m-1}}\}$$

to be a subsequence of S that we can further split into two subsequences of the same size $(q - 1)/2$, say

$$A_1 = \{x^{i_0}y^{a_0}, x^{i_0}y^{a_2}, \dots, x^{i_0}y^{a_{m-2}}\} \cup \{x^{i_0}y^{a_1}, x^{i_0}y^{a_3}, \dots, x^{i_0}y^{a_{m-1}}\},$$

satisfying $a_0 \not\equiv a_2 \pmod{q}$ and $a_1 \not\equiv a_3 \pmod{q}$. Since s^{i_0} generates \mathbb{Z}_q^* , s^{2i_0} generates the quadratic residues of \mathbb{Z}_q^* . From Corollary 3.10, there exist two permutations σ of $(0, 2, \dots, m-2)$ and τ of $(1, 3, \dots, m-1)$ such that

$$\begin{aligned} 1 &\equiv a_{\sigma(0)} + a_{\sigma(2)}s^{2i_0} + \dots + a_{\sigma(m-2)}s^{(m-2)i_0} \pmod{q}, \\ -1 &\equiv a_{\tau(1)}s^{i_0} + a_{\tau(3)}s^{3i_0} + \dots + a_{\tau(m-1)}s^{(m-1)i_0} \pmod{q}. \end{aligned}$$

Therefore

$$\begin{aligned} 1 &= y \cdot y^{-1} = y^{a_{\sigma(0)} + a_{\sigma(2)}s^{2i_0} + \dots + a_{\sigma(m-2)}s^{(m-2)i_0}} \cdot y^{a_{\tau(1)}s^{i_0} + a_{\tau(3)}s^{3i_0} + \dots + a_{\tau(m-1)}s^{(m-1)i_0}} \\ &= x^{i_0}y^{\sigma(0)} \cdot x^{i_0}y^{\tau(1)} \cdot x^{i_0}y^{\sigma(2)} \cdot x^{i_0}y^{\tau(3)} \dots x^{i_0}y^{\sigma(m-2)} \cdot x^{i_0}y^{\tau(m-1)}, \end{aligned}$$

thus S is not free of product-1 subsequences.

(3.2) **Subcase $q \equiv 3 \pmod{4}$ and $q \geq 7$:** It is known that -1 is not a quadratic residue modulo q . Let

$$A_1 = \{x^{i_0}y^{a_0}, x^{i_0}y^{a_1}, \dots, x^{i_0}y^{a_{m-1}}\},$$

where at least 3 of the a_j 's are distinct. By considering the set of all products obtained by changing the order of the elements of A_1 , we obtain the set

$$\begin{aligned} \mathcal{C} &= \{\alpha_\pi = a_{\pi(0)} + a_{\pi(1)}s^{i_0} + \dots + a_{\pi(m-1)}s^{(m-1)i_0} \in \mathbb{Z}_q \mid \\ &\quad \pi \text{ is a permutation of } (0, 1, \dots, m-1)\}. \end{aligned}$$

Hence, it is enough to consider the exponents α_π of y . Reindexing the a_j 's, we may construct the set of exponents

$$\begin{aligned} X &= \{s^{2ni_0}(a_0 + a_2s^{2i_0} + \dots + a_{m-2}s^{i_0(m-2)}) \in \mathbb{Z}_q \mid 0 \leq n \leq m-1\}, \\ Y &= \{s^{2ni_0}(a_1s^{i_0} + a_3s^{3i_0} + \dots + a_{m-1}s^{i_0(m-1)}) \in \mathbb{Z}_q \mid 0 \leq n \leq m-1\}, \end{aligned}$$

where X and Y each have at least 2 distinct elements. Clearly, $X + Y \subset \mathcal{C}$. Suppose that $0 \notin X + Y$ (otherwise we are done). By Lemma 3.4, $|X + Y| = m$, thus $X + Y = \mathbb{Z}_q^*$. By Lemma 3.5, we may assume without loss of generality that $|X| = m/2$ and $|Y| = m/2$. Let

$$\alpha = a_0 + a_2 s^{2i_0} + \cdots + a_{m-2} s^{i_0(m-2)} \in A.$$

If $-\alpha \in Y$ then $0 \in X + Y$, a contradiction. Therefore $-\alpha \in X$. Hence, there exists $0 \leq n \leq m-1$ such that $\alpha s^{2ni_0} \equiv -\alpha \pmod{q}$, which implies $s^{2ni_0} \equiv -1 \pmod{q}$, so -1 is a quadratic residue modulo q , but this is impossible. □

Acknowledgements. We would like to thank the anonymous “user44191” from the *Math Overflow Forum* (<http://mathoverflow.net/>) for providing a hint for solving Lemma 3.6. The second author would like to thank CAPES/Brazil for the PhD student fellowship.

REFERENCES

- [1] Bass, J.; *Improving the Erdős-Ginzburg-Ziv theorem for some non-abelian groups*. J. Number Theory **126** (2007), 217-236.
- [2] Bialostocki, A., Dierker, P.; *On the Erdős-Ginzburg-Ziv theorem and the Ramsey numbers for stars and matchings*. Discrete Math. **110** (1992), 1-8.
- [3] Caro, Y.; *Zero-sum problems – A survey*. Discrete Mathematics **152**, (1996) 93-113.
- [4] Erdős, P., Ginzburg, A., Ziv, A.; *Theorem in the additive number theory*. Bull. Res. Council Israel **10** (1961) 41-43.
- [5] Gao, W., Geroldinger, A.; *On long minimal zero sequences in finite abelian groups*. Period. Math. Hungar. **38** (3) (1999), 179-211.
- [6] Gao, W., Geroldinger, A.; *On zero-sum sequences in $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$* . Integers: Electronic Journal of Combinatorial Number Theory **3** (2003), #A8.
- [7] Gao, W., Geroldinger, A.; *Zero-sum problems in finite abelian groups: a survey*. Expo. Math. **24** (2006), 337-369.
- [8] Gao, W., Geroldinger, A., Gryniewicz, D. J.; *Inverse zero-sum problems III*. Acta Arithmetica. **141.2** (2010), 103-152.
- [9] Gao, W., Geroldinger, A., Schmid, W. A.; *Inverse zero-sum problems*. Acta Arithmetica. **128.3** (2007), 245-279.
- [10] Gao, W., Lu, Z.; *The Erdős-Ginzburg-Ziv theorem for dihedral groups*. J. Pure Appl. Algebra **212** (2008), 311-319.
- [11] Ireland, K., Rosen, M.; *A Classical Introduction to Modern Number Theory*. Second Edition, (1990).
- [12] Nathanson, M. B.; *Additive Number Theory*. Springer, New York (1996).
- [13] Olson, J.; *A combinatorial problem on finite Abelian groups I*. J. Number Theory **1** (1969), 8-10.
- [14] Olson, J.; *A combinatorial problem on finite Abelian groups II*. J. Number Theory **1** (1969), 195-199.
- [15] Olson, J., White, E. T.; *Sums from a sequences of group elements*. in: Number Theory and Algebra, Academic Press, New York, (1977), 215-222.
- [16] Reiher, C.; *A proof of the theorem according to which every prime number possesses Property B*. Ph.D. thesis, University of Rostock (2010). Available at http://ftp.math.uni-rostock.de/pub/preprint/2010/pre10_01.pdf.
- [17] Schmid, W. A.; *Inverse zero-sum problems II*. Acta Arith. **143** (2010), no. 4, 333-343.
- [18] Schmid, W. A.; *The inverse problem associated to the Davenport constant for $C_2 \oplus C_2 \oplus C_{2n}$, and applications to the arithmetical characterization of class groups*. The Electronic Journal of Combinatorics **18** (2011), #P33 477-487.
- [19] Vosper, A. G.; *The critical pairs of subsets of a group of prime order*. J. London Math. Soc. **31** (1956), 200-205.
- [20] Zhuang, J., Gao, W.; *Erdős-Ginzburg-Ziv theorem for dihedral groups of large prime index*. European J. Combin. **26** (2005), 1053-1059.

DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDADE FEDERAL DE MINAS GERAIS, UFMG, BELO HORIZONTE, MG, 30123-970, BRAZIL,

E-mail address: fbrocher@mat.ufmg.br

E-mail address: savio.ribas@gmail.com